Amendments to the Specification:

Please replace the paragraphs extending from page 3, line 18 to page 5, line 12 with the following new paragraphs:

Turning now to the drawings, FIG 1 illustrates a conventionally implemented wireless network to emphasize the associated security concerns. In the depicted embodiment, wireless 20 network **100** includes a set of wireless client devices **102A** through **102N** (generically or collectively referred to herein as wireless client(s) **102).** Each wireless client **102** represents some form of a data processing device such as a desktop personal computer, a notebook computer, personal digital assistant (PDA), pocket PC, paging device, and so forth. Each client **102** communicates information to and receives information from a wireless access point (WAP) **104**. WAP **104** is connected to a wired network medium **107** that is connected to a wide area network (WAN) **110** such as the Internet via gateway **106**. Network medium **107** may also connect WAP with one or more wired clients (not depicted), local area networks, and other WAP's.

WAP **104** may be compliant with a wireless LAN standard or protocol such as ~~the Bluetooth~~ BLUETOOTH® wireless technology standard or one of the IEEE 802.11 standards. In such an embodiment, WAP **104** [[is]] creates a one-to-many connection in which multiple clients **102** communicate through the WAP **104** to effectively share the bandwidth of network medium **107.** In many respects, this one-to-many functionality is highly desirable and beneficial. In a typical household or small business, for example, the cost of access to a high speed embodiment of network medium **107** may limit most users to a single connection. In such cases, the household or small business can effectively share the single connection using WAP **104** and some relatively inexpensive adapter hardware.

With respect to the increasingly important considerations of network security and privacy, however, schematically represented in FIG. 1 by pirate **105**, WAP **104** is the cause of significant concern. As conceptually illustrated in FIG 1, WAP **104** has an effective range or radius, within which any suitably configured wireless adapter can unilaterally "attach" to the wireless LAN. Such unauthorized users may then send or receive network packets usually without the knowledge of authorized clients **102.** Considering that many wireless adapter cards and technologies currently specify an effective range approaching 1000 feet, the potential for unauthorized users attaching to a WAP is quite great. Thus, one of the great attributes of WAP **104,** the ability of connect multiple users to the network is also one of its principal drawbacks. Moreover, the configuration or setup required to implement even a simple implementation of **WAP 104** is not trivial. Entire texts are dedicated to the topic of wireless LAN's and the configuration of access points with particular emphasis being placed on security.

The present invention addresses the problems inherent in the one-to-many design of WAP **104** by enabling a simple wireless implementation suitable for use with a single device and a corresponding wired network port. Referring now to FIG 2, selected elements of a wireless data processing assembly **221** according to one embodiment of the present invention are depicted. Data processing assembly **221** as depicted in FIG 2 includes a client device **202** in the form of a microprocessor based data processing system. Client [[**103**]] **202** includes one or more general purpose microprocessors **220A** through **220N**

(generically or collectively referred to herein as microprocessor(s) **220**) sharing a common system memory **224** over a system bus **222** in a symmetrical multiprocessing arrangement that will be familiar to those in the field of computer architecture.

An I/O bridge **226** enables peripheral devices of client [[**103**]] **202** to communicate with processors **220** and system memory **224** one or more peripheral busses, one of which is indicated by reference numeral **228.** I/O bus **228** is likely compliant with an industry standard peripheral **30** bus such as the Peripheral Components Interface (PCI) local bus that is widely implemented and well known in the field. Among the most common type of peripheral adapters connectable to peripheral bus **228** is a network communication device, also sometimes referred to as a network interface device or NIC **230.** NIC **230** likely includes a port such as an RJ-45 port for receiving a wired connector. In one embodiment desirable for its compatibility with a very large number of LAN configurations, NIC **230** is an Ethernet compliant NIC that includes a standard RJ-45 connector port **231.** In a conventional wired LAN configuration, port **231** receives an RJ-45 connector through which a suitable cable, e.g., a Category 5 or CAT 5 cable as specified by the Electronics Industries Association (EIA), provides the network medium to client [[**103**]] **202.** It is worth noting for the sake of comparison that, in a conventional wireless LAN using a WAP **104** as shown and described with respect to FIG 1, the LAN connection is typically implemented using a wireless adapter card. Such a wireless adapter card may be in the form of a PCI, PCMIA or other suitable adapter type. Regardless of its form factor, a conventional wireless adapter is a distinct device that is different than and unconnected to NIC **230.**

Please replace the paragraph extending from page 5, line 20 to page 6, line 3 with the following new paragraph:

According to the present invention, a dedicated, secure, and wireless communication line (conceptually represented by reference numeral **233**) is established between client **202** and network medium **107** using the pair of wireless bridge devices **232A** and **232B.** In one embodiment, wireless bridge devices **232A** and **232B** are handheld devices that include RJ-45 connectors via which devices **232A** and **232B** may be "plugged" into ports **231** and **234.** In the preferred embodiment, communication link **233** is established by merely plugging devices **232A** and **232B** into their respective ports assuming that appropriate sources of power are available to bridge devices **232.** This preferred embodiment implies that bridge devices **232A** and **232B** include facilities and functionality to establish link **233** between themselves and that no additional resources, either software or hardware, are required of client [[**103**]] **202** and network medium **107** to establish the link. In other words, if a suitable wired medium, if client [[**103**]] **202** and network medium **107** are configured wherein a CAT 5 cable (not depicted) connected to ports **231** and **234** provides a wired link between client [[**103**]] **202** and network medium **107,** the cable could then be replaced by wireless bridge devices **232A** and **232B** to establish wireless link **233** without reconfiguration of client [[**103**]] **202** or network medium **107.**

Please replace the paragraph extending from page 6, line 12 to page 7, line 2 with the following new paragraph:

> As depicted in FIG 3B, encode unit **340** of bridge device **232A** includes an encryption unit **350** that encrypts outgoing data according to a predetermined encryption algorithm using an encryption key **352.** The encrypted information is then passed to a wireless protocol layering **15** unit **355** that formats the encrypted packet according to any of several standardized wireless protocols or according to a proprietary protocol. In one embodiment, for example, wireless protocol layering unit **355** implements ~~a Bluetooth~~ BLUETOOTH® wireless technology and adds a corresponding protocol layer to the encrypted packet produced by encryption unit **350.** The encrypted and formatted packet is then suitable for transmission via the wireless link **233** using the wireless transmit facilities indicated by reference numeral **344** of FIG 3A. At the receiving end of wireless link **233,** bridge device **232B** includes wireless protocol ~~processing~~ layering unit **365** that extracts the encrypted data from each incoming packet and forwards the encrypted packet to a decryption unit **360.** Decryption unit **360** uses a decryption key **362** that is matched to the encryption key **352** of wireless bridge **232A** to decode incoming packets. Importantly, the encryption/decryption keys **352/362** of each pair of bridge devices **232A** and **232B** is unique to that bridge pair. Thus, the wireless bridge devices in a device pair **232A/1232B** are designed to communicate with each other exclusively. In one embodiment, the encryption/decryption keys **352/362** in are static and physically encoded or burned into encode and decode units **340** and **342.** In other embodiments, the wireless bridge pair **232A / 232B** alters the encryption keys in use from time to time either automatically or upon request. In such embodiments, a strong authentication algorithm verifies the encryption keys after each key change to ensure that the bridge pair **232A** *1* **232B** is capable of communicating with each other at all times.